УДК 004.056

Н. Р. Кондратенко
В. С. Мідзяєв

ВИЯВЛЕННЯ АНОМАЛІЙ НА ОСНОВІ ТЕХНОЛОГІЇ САМООРГАНІЗАЦІЇ

Вінницький національний технічний університет

Анотація: *у даній роботі проведено аналіз методу виявлень аномалій на основі технології самоорганізації за допомогую кластеризації.Розглянуто спосіб прийнятя рішення на основі даного методу.*
Ключові слова: *Кластеризація, трафік, виявлення аномалій, зловживання.*

Abstract: *This paper analyzes the method of detection of anomalies technology based on self dopomohuyu clustering. The way to make a decision based on this method.*
Keywords*: Clustering, traffic, anomaly detection, abuse.*

Інформаційні технології все більше проникають у всі сфери людської діяльності. Інформація може представляти велику цінність та бути предметом купівлі-продажу. Здебільшого саме через це інформаційні ресурси стають об'єктом атаки з метою їх заволодіння. Це призводить до того, що актуальним стає питання захисту. У зв'язку зі збільшенням обсягів інформації, що циркулюють в локальних обчислювальних мережах, та розширенням спектра завдань, що вирішуються за допомогою інформаційних систем, виникає проблема, пов'язана зі зростанням числа загроз і підвищенням вразливості інформаційних ресурсів [1].

Методи виявлення атак в сучасних системах недостатньо опрацьовані в частині формальної моделі атаки, і, отже, для них досить складно строго оцінити такі властивості, як обчислювальна складність, коректність, завершеність і т.д. Прийнято розділяти методи виявлення атак на методи виявлення аномалій і методи виявлення зловживань. Зловживання – це такий тип атак, у яких використовуються відомі недоліки інформаційних систем. Аномалія – це незвичайна активність в цілому, що може свідчити про вторгнення. Якщо зафіксована активність користувача відрізняється від очікуваної поведінки, то говорять про аномалію.

Створення ефективних підходів до захисту інформаційних систем зіштовхується також із браком обчислювальної потужності. З самого початку розвитку комп'ютерів і комп'ютерних мереж спостерігаються дві тенденції – щорічне подвоєння продуктивності обчислювачів, доступних за одну й ту ж вартість, та потроєння пропускної спроможності каналів зв'язку за той же період. Таким чином, зростання обчислювальної потужності вузлів мережі відстає від зростання обсягів переданої по мережі інформації, що з кожним роком посилює вимоги до обчислювальної складності алгоритмів систем захисту інформації [2].

При побудові системи виявлення аномалій використано нейромережну модель. До основних переваг отриманої моделі можна віднести те, що навчивши систему, вона узагальнює цю інформацію та формує очікувану реакцію у подібних ситуаціях. Паралельна обробка інформації у нейромережних системах дозволяє створювати достатньо швидкодіючі чи навіть он-лайн системи. В процесі навчання нейромережна система дає можливість виділяти ті найважливіші ознаки дій користувачів чи зловмисників, які формують базу для прийняття рішень. Ще однією важливою перевагою нейромережної моделі системи виявлення аномалій є можливість прогнозування роботи системи на основі її минулих дій. Нейромережна система виявлення аномалій будується таким чином, що на її вхід подається набір параметрів, які характеризують роботу системи, а на виході отримуємо два кластера, білий та чорний, що характеризує наявність чи відсутність аномалій у її роботі. За вхідні параметри можуть бути використані час роботи користувача, які програми він використовує найбільше, швидкість набору команд і т.п. Такий підхід дає можливість не тільки виявляти аномалії, але й проводити ідентифікацію користувачів [5].

У даній статті розглянутий підхід до побудови системи виявлення вторгнень. Показано, що аналіз дій користувача є одним із ефективних засобів виявлення зловмисника у комп'ютеризованих

системах. Як інструмент при реалізації даної системи використані штучні нейронні мережі. За допомогою кластерів, користувачу надається змога краще оцінити стан мережі та прийняти правильне рішення. За допомогою розподілення на 2 кластери, білий - нормальний режим роботи та чорний – аномальний, можна приймати рішення щодо даної ситуації. Таким чином, сьогодні потрібно використовувати кластеризацію, адже це є ефективно і допомагає для нормальної роботи мережі.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Ryan J. Intrusion Detection with Neural Networks / Ryan J., Lin M.-J., Miikkulainen R. // Advances in Neural Information Processing Systems. – Cambridge, MA : MIT Press, 1998. – P. 254-272.
2. Большев А.К. Подход к обнаружению аномального трафика в компьтерных сетях с использова- нием методов кластерного анализа / А.К. Большев, В.В. Яновский // Известия Государственного Электротехнического Университета, серия Информатика, управление и компьютерные технологии. –2006. – Выпуск 3/2006. – Изд-во СПбЭТУ, СПб. – С. 38-45.
3. Котенко И.В. Перспективные направления исследований в области компьютерной безопасности /И.В. Котенко, Р.М. Юсупов // Защита информации. Инсайд. 2006. – № 2. – С. 46-57.
4. Denning D. An Intrusion Detection Model / D. Denning // IEEE Transactions on Software Engineering. –1987. – V. SE-13, № 1. – P. 222-232.
5. Головко В.А. Нейронные сети: обучение, организация, применение / В.А. Головко // Нейрокомпью- теры и их применение : [учеб. пособие]. – М., 2001. – – 256 с
6. Виявлення мережевих аномалії на основі нейромережевих технологій. [Електронний ресурс]. – Режим доступу до ресурсу: http://ua.nauchebe.net/2015/04/viyavlennya-merezhevix-anomali%D1%97-na-osnovi-nejromerezhevomu-texnologij/- назва з екрану.
7. Кондратенко Н. Р., Куземко С. М. Основи нейромереж. Теорія і практика. Навчальний посібник, ВНТУ. – 2006.

Мідзяєв Вадим Сергійович, студент, Вінницький національний технічний університет, м. Вінниця, факультет інформаційних технологій та комп'ютерної інженерії, 1БС-12б, vadim14121993@gmail.com

Кондратенко Наталя Романівна, к.т.н., професор кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця.

Midziayev Vadym Serhiyovych , student, Vinnytsia National Technical University, Vinnytsia, Faculty for Information Technologies and Computer Engineering, 1BS-12b, vadim14121993@gmail.com

Kondratenko Natalya Romanivna, Ph.D. professor of Vinnytsia National Technical University, Vinnytsia, Faculty for Information Technologies and Computer Engineering, chair of information security.